NATIONAL DEFENSE UNIVERSITY

NATIONAL WAR COLLEGE

READY OR NOT, U.S. INFORMATION OPERATIONS

JOHN M. MACKIN
5605
DOING NATIONAL MILITARY STRATEGY

PROFESSOR
COL JIM HARRIS

ADVISOR
DR. DAVID ROSENBERG

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2002		**00-00-2002 to 00-00-2002**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Ready or Not, U.S. Information Operations	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National War College,300 5th Avenue,Fort Lesley J. McNair,Washington,DC,20319-6000**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT
see report

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**14**	

READY OR NOT, U.S. INFORMATION OPERATIONS

Reliance upon information technology has increased significantly over the past few years and continues to rapidly expand across the globe. According to Moore's Law, microprocessor speeds are hypothesized to double every 18 months.[1] Increases in processing speed, reduced cost, and greater availability all contribute to the growth in information technology dependence. It would be very difficult for the majority of the world to get through the day without having the ability to turn on a computer and access the Internet. The information age is upon us.

The importance of maintaining control of information has increased proportionally with the dependence upon using the systems. The term "information operations" was developed to focus the U. S. military on the importance of information in this new era. Information operations are defined as "actions taken to affect adversary information and information systems while defending one's own information and information systems".[2] The most recently published National Security Strategy, written during President Clinton's term, states, "we are committed to maintaining information superiority—the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting and/or denying an adversary's ability to do the

[1] Accessed at www.intel.com/research/silicon/mooreslaw.htm.

[2] Joint Chiefs of Staff, "Joint Policy on Information Operations-JCS PUB 3-13", October 1998, Pg. Vii.

same".[3] Joint Vision 2020 states, "The continued development and proliferation of information technologies will substantially change the conduct of military operations. These changes in the information environment make information superiority a key enabler of the transformation of the operational capabilities of the joint force."[4] For at least the last 4 years, the Department of Defense has obligated money towards ensuring the U.S. military is prepared to conduct information operations. This paper attempts to determine whether or not the U.S. military is ready to conduct information operations.

Just what are information operations? "Theoretical concepts of war in cyberspace at the one end of the spectrum, and the pragmatic development of the limited concept of Command and Control Warfare (C2W) at the other, have now matured into the regularly redefined integrating strategy of Information Operations."[5] Information Operations, according to JCS Pub 3-13, are divided between offensive capabilities and defensive capabilities. The offensive capabilities "include, but are not limited to, operations security (OPSEC), military deception, psychological operations (PSYOPS), electronic warfare (EW), physical attack/destruction, and special information operations

---

[3] White House, "A National Security Strategy for a New Century", December 1999, Pg. 12.

[4] Joint Chiefs of Staff, "Joint Vision-2020," Pg. 3.

[5] Andrew Garfield, "Information Operations as an Integrating Strategy: The Ongoing Debate," Cyberwar 3.0, Pg. 261.

(SIO), and may include computer network attack."[6] Defensive information operations include: "information assurance, OPSEC, physical security, counter deception, counterpropaganda, counterintelligence, EW, and SIO."[7]

With the exception of computer network attack, the functions listed under offensive information operations are functions that the military has performed time and time again. Examples of OPSEC, military deception, PSYOPS, EW, and physical attack can be drawn from almost any military conflict. Specific joint doctrine provides guidance over the following functions:

OPSEC	JCS Pub 3-54 Joint Doctrine for Operations Security
Deception	JCS Pub 3-58 Joint Doctrine for Military Deception
PSYOPS	JCS Pub 3-53 Doctrine for Joint PSYOPS
EW	JCS Pub 3-51 Joint Doctrine for EW

Physical destruction is, of course, the main element of military force and is included throughout doctrine. The importance of these functions, although not always practiced, is well understood.

The same can be said for the pillars of defensive Information Operations. The attack on the USS COLE heightened OPSEC awareness and increased the requirement for improved physical security. The importance of defending oneself or critical information against an attack, whether through physical attack, EW, propaganda, intelligence collection, or cyber means, is also well understood. The same doctrine identified in the

---

[6] Joint Chiefs of Staff, "Joint Policy on Information Operations-JCS PUB 3-13," October 1998, Pg. Viii.

[7] Ibid. Pg Viii.

previous paragraph provides the guiding principles to ensure the pillars of defensive Information Operations are effectively carried-out.

It is no coincidence that the "conventional" aspects of information operations match directly with the focus behind C2W. "C2W is the integrated use of PSYOP, military deception, OPSEC, EW, and physical destruction."[8] Specific training has been provided to U.S. enlisted personnel and officers making them experts in each of these fields. Equipment has been procured to ensure U.S. maintains supremacy in each of these areas. The legal aspects of each of these pillars are also understood. Information operations evolved from the C2W concept by adding the cyber domain. The U.S. is certainly capable and ready, as evidenced by DESERT STORM, to conduct C2W operations, but in order to be ready to conduct information operations it must also be prepared to conduct war in the cyber domain.

First, on the offensive cyber front of Information Operations, computer network attack is certainly technologically feasible. Computer hackers carry out computer network attacks daily. The tools required to conduct these attacks are readily available throughout the Internet for free. All one needs is a computer and limited expertise to conduct a computer attack and wage cyber war.

The U.S. understands that computer network operations (computer network attack and defense) are pertinent aspects of

---

[8] JCS Pub 3-13.1, "Joint Doctrine for Command and Control Warfare," 7 February 1996, Pg. V.

future wars and certainly has the technology and expertise to carry out attacks. In October 2000, U.S. Space Command took charge of computer network attack (CNA). The Joint Task Force-Computer Network Defense was renamed the Joint Task Force-Computer Network Operations and subordinated to U.S. Space Command. "As with any military capability, the U.S. will only employ CNA after careful policy and legal review."[9] The legal issue is significant and complex. U.S. CNA can be classified into two scenarios: attacks during war and retaliatory operations following a computer network attack against U.S. assets.

If an attack was carried out against a country in which the U.S. was at war with, the CNA against the enemy nation could be legal. However, "By treaty and longstanding customary law, the territory of neutral states is supposed to be inviolable by the forces of belligerents."[10] This means that if an attack crosses through or uses a neutral nation's network then it would infringe on that neutral nation's territory. The attack could be considered illegal and an act of war against the neutral nation. Additionally, if the neutral nation did nothing to resist the passing of the attack then it could become a legitimate target of the attacked country. The law when originally written never envisioned a world connected via a

---

[9] Space Daily, "US Space Command Takes Charge of Computer Network Attack," 2 October 2000, Pg. 1.

[10] Lawrence T. Greenberg, Seymour E. Goodman, Kevin J. Soo Hoo, "Information Warfare and International Law," 1998, Pg. 26.

global network. Therefore, the question ends up being whether a CNA that uses a neutral nation's network is considered a physical event. If it is, then it is illegal. If it is not, then it is legal. International law has not yet resolved these ambiguities.

In the case where the U.S. has been attacked and has determined that retaliation is in order, the law is even more pertinent. "A government cannot respond to an attack successfully unless it can identify the attack's source."[11] Sources of attacks can come from an individual, a group, or a nation. Identifying this source is not easy. Usually the only indicator of the attacker is an Internet Protocol (IP) address. Attackers have the capability to mask their true identity or conduct attacks through multiple innocent IP addresses.

Besides determining who conducted the attack, one must prove that the act was nationally sponsored before retaliation in or against another country can commence. National sponsorship could prove even more difficult to pin down. However, this does not differ much from the work being done to tie terrorist groups to nations that support them. Intelligence sources certainly will play a significant role in determining the legality of a retaliatory strike, whether via physical means or cyber means.

The majority of the computer incidents will initially be handled by law enforcement means. Cooperation between nations, and the extradition of individuals are the most probable since

---

[11] Ibid. Pg. 72.

absolute proof is difficult to obtain. However, depending on the level of cooperation with possible suspect nations, the U.S. may decide to conduct an attack, possibly covertly.

"International law leaves space for the U.S. and others to conduct information warfare activities, perhaps even in peacetime, without significant legal repercussions."[12] However, the unresolved legal ambiguities coupled with the difficulty in identifying culprits make it difficult to "pull the trigger". International treaties regarding the use of the global network and mutual cooperation in identifying culprits are certainly needed to allow the U.S. to use CNA more readily. However, treaties and laws will not stop individuals and groups who have little regard for international law from carrying-out attacks.

Because of this, a good, effective defense (information assurance) is paramount. The threat is real. Individuals, groups, and state sponsored elements pose a threat not only to the U.S. military, but also U.S. critical infrastructure. "We (China) should formally turn nonmilitary activities such as computer hacking, financial intrusion, and media propaganda into methods of warfare and form a many-stranded "combination of non-restriction" with the aim of defeating the enemy and winning victory."[13]

---

[12] Ibid. Pg. 93.

[13] Unrestricted Warfare, Qiao Liang and Wang Xiangsui, PLA Literature and Arts Publishing House, February 1999 accessed at www.terrorism.com/infowar/index.shtml.

Dr. Hamre, former Under Secretary of Defense, recognized the necessity for a good defense in order to maintain the capability to process information uninterrupted. He developed the "layered defense" approach and implemented it across the Department of Defense. Millions of dollars have been spent on firewalls and intrusion detection software. Individual services stood up missions, Naval Computer Incident Response Team (NAVCIRT) and Air Force Computer Emergency Response Team (AFCERT), responsible for overseeing computer networks. However, this has not proven to be enough. "In 1995, the Defense Information Systems Agency estimated 250,000 attacks by hackers on the Pentagon's unclassified systems—and 160,000 successful entries."[14] The "I Love You" virus inconvenienced most of the Department of Defense computer systems.

To be able to deter computer terrorists from wanting to attack systems is what is truly desired. All efforts should be made to effect deterrence. The Russians have taken this to an extreme by threatening nuclear retaliation if they are subject to an information attack.[15]

"Nations and non-state actors that do not operate under "Western values" see a passive posture as a sign of weakness that creates targets of opportunity."[16] The U. S. must be

---

[14] M.J. Zuckerman, "Post-Cold War Hysteria or a National Threat", USA Today, June 5, 1996.

[15] Stephen Blank, "Russia's Armed Forces on the Brink of Reform", October 1997 accessed at www.fas.org/nuke/guide/russia/agency/RussiasArmedForcesontheBrinkofReform.htm.

[16] Arnaud de Borchgrave, Frank J. Cilluffo, Sharon L. Cardash, Michele M. Ledgerwood, "Cyber Threats and Information Security—Meeting the 21st Century Challenge", May 2001, Pg. 28.

prepared to forcibly stop, whether it is via covert or overt methods, attacks against key computer systems. Preferably, the capability should be developed to perform an immediate retaliatory strike when an attack is attempted. The computer that is being used to attempt the attack, whether or not the attack is successful or not, should be accessed for evidence and possibly destroyed. Again, this is difficult in that one is not always immediately sure who is performing the attack. If technologically feasible this “hack-back” should be attempted in order to gain evidence that the computer in question actually conducted the attack. The ability to damage or destroy the computer immediately serves as a good deterrent.

CNA becomes a significant deterring agent. In order to “assure” information defense is important, but the ability to deter attacks is even more beneficial. In order to effectively deter an attack via computer means the issues previously identified in the retaliatory CNA section of the paper must first be overcome.

In conclusion, the U.S. is and has been ready to conduct C2W. Much work has been accomplished in preparing the Department of Defense to perform information operations in the complete sense. However, if both offensive and defensive information operations are to be effective more has to be done to enable CNA to be performed whenever necessary. The ambiguities surrounding international law must be clarified. Coalitions must be established that promote a common understanding of when CNA is legal and against which targets it

may be performed. Technology must be enhanced to fingerprint the attacker immediately and enable a counter-attack. This ability will not only assist with retaliatory offensive operations, but also promote a more thorough defense of information in the quest to achieve and maintain information superiority.

Executive Summary

Is the U.S. military prepared to conduct information operations? The term “information operations” is defined. Information operations are divided into offensive and defensive categories, but it can also be divided into command and control warfare (C2W) and computer related functions. The U.S. military knows how to and is ready to conduct C2W. Examples of effective C2W can be found in many, if not all, recent conflicts. Doctrine has been developed to perform all the elements of C2W, but it has not been developed to perform Computer Network Attack or effective information assurance.

Since the U.S. military understands and has performed C2W, then in order to be ready to conduct information operations the nation must also be ready to conduct computer network attack and information assurance. It is shown that legal ramifications and technological difficulties in identifying attackers hinder the ability to perform effective computer network attacks. It is also demonstrated that the current policy of defense-alone is not enough to “assure” U.S. information. Attackers must be deterred through retaliatory attacks.

In conclusion, the U.S. is not quite ready to conduct information operations. Until international legal ambiguities are resolved, coalitions built, and technological fixes put in place that can immediately identify attackers, CNA will not be able to be used as required. Until CNA can be effectively used, the ability to deter attacks is limited and the quest to maintain information superiority jeopardized.

Bibliography

Andrew Garfield, "Information Operations as an Integrating Strategy: The Ongoing Debate," *Cyberwar 3.0*, October 2000.

Arnaud de Borchgrave, Frank J. Cilluffo, Sharon L. Cardash, Michele M. Ledgerwood, "Cyber Threats and Information Security—Meeting the 21st Century Challenge", May 2001.

George Stein, "US Information Warfare", *Jane's Special Report*, 1996.

Intel Corp., "Moore's Law," accessed at www.intel.com/research/silicon/mooreslaw.htm.

Joint Chiefs of Staff, "Joint Policy on Information Operations-JCS PUB 3-13," October 1998.

Joint Chiefs of Staff, "Joint Doctrine for Command and Control Warfare-JCS PUB 3-13.1," February 1996.

Joint Chiefs of Staff, "Joint Doctrine for Electronic Warfare-JCS PUB 3-51," 7 April 2000.

Joint Chiefs of Staff, "Doctrine for Joint Psychological Operations-JCS PUB 3-53," 10 July 1996.

Joint Chiefs of Staff, "Joint Doctrine for Operations Security-JCS PUB 3-54," 24 January 1997.

Joint Chiefs of Staff, "Joint Doctrine for Military Deception-JCS PUB 3-58," 31 May 1996.

Joint Chiefs of Staff, "Joint Vision-2020"

Lawrence T. Greenberg, Seymour E. Goodman, Kevin J. Soo Hoo, "Information Warfare and International Law," 1998.

M.J. Zuckerman, "Post-Cold War Hysteria or a National Threat", USA Today, June 5, 1996.

Potomac Institute for Policy Studies, "Seminar on Cyber-Terrorism and Information Warfare: Threats and Responses", 16 April 1998.

Qiao Liang and Wang Xiangsui, "Unrestricted Warfare," PLA Literature and Arts Publishing House, February 1999 accessed at www.terrorism.com/infowar/index.shtml.

Roger C. Morlander, Andrew S. Riddile, Peter A. Wilson, "Strategic Information Warfare: A new Face of War", 1996 RAND, accessed at www.rand.org/publications/MR/MR661/MR661.html.

Space Daily, "US Space Command Takes Charge of Computer Network Attack," 2 October 2000.

Stephen Blank, "Russia's Armed Forces on the Brink of Reform", October 1997 accessed at www.fas.org/nuke/guide/russia/agency/RussiasArmedForcesontheBrinkofReform.htm.

Steven J. Tomisek, Strategic Forum, "Homeland Security: The New Role for Defense," February 2002.

U.S. GAO, "Combating Terrorism: Selected Challenges and Related Recommendations," September 2001.

White House, "A National Security Strategy for a New Century," December 1999.